REMARKS

The status of the claims 1-5, 7-11, 20-29, 41-42, 49-53, 55-67 and 76-79 is as indicated above. Claims 49 and 76 have been amended per this Response. The Applicant respectfully requests that this application be allowed and forwarded on to issuance.

§ 102 Rejections

Claims 1-5, 7-11, 20-29, 41-42, 49-53, 55-67 and 76-79 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent Application Publication No. 2002/0172368 ("Peterka").

The Claims

Claim 1 recites a method comprising [emphasis added]:

- receiving a request to transfer application data from a source computing device to a destination computing device;
- checking whether the application data can be transferred to the destination computing device, and if so, then checking whether the application data can be transferred under control of a user or a third party, wherein checking whether the application data can be transferred comprises checking a type of the application data, ***the type of the application data being one of non-migrateable, user-migrateable, and third party-migrateable***; and
- receiving input from the appropriate one of the user or third party to control transferring of the application data to the destination computing device.

In making out the rejection of this claim, the Office argues that its subject matter is anticipated by Peterka. Applicant respectfully disagrees and traverses the Office's rejection.

Specifically, Peterka fails to disclose checking a type of the application data, the type of the application data being one of non-migrateable, user-

migrateable, and third party-migrateable, as recited in this claim. More particularly, Peterka fails to disclose application data being of a **non-migrateable** type.

The Specification at page 29, lines 12-17, instructs as follows:

> "Non-migrateable secrets ... are unconditionally non-migrateable – they cannot be transferred to another computing device. Non-migrateable secrets ... are encrypted by an encryption algorithm that uses, as an encryption key, non-migrateable key .... The trusted core will not divulge non-migrateable key ... to another computing device, so no other device will be able to decrypt trusted application secrets ...."

Peterka, on the other hand, is directed to providing free program previews and/or other program content to clients, wherein encryptions keys are used to control client viewing (Abstract of Peterka). More to the point, Peterka is directed to disseminating program content to authorized (paying) clients. Peterka is completely devoid of any teachings directed to **non-migrateable** application data in any way or for any purpose as, under Peterka, all program content (arguably, "data") is migrateable to some authorized recipient(s). In fact, Peterka *teaches directly away* from the concept of **non-migrateable** application data, as Peterka is directed to providing (selling) any and all program content to as many clients as possible – see paragraph 0005 of Peterka.

For at least the foregoing reasons, claim 1 is allowable.

Claims 2-5 and 7-11 are allowable as depending from an allowable base claim.

Claim 20 recites one or more computer readable media having stored thereon a plurality of instructions that, when executed by one or more

processors of a source computing device, causes the one or more processors to [emphasis added]:

- receive a request to transfer an application secret from the source computing device to a destination computing device;
- identify a type of the application secret;
- ***if the type is non-migrateable, then not allow the application secret to be transferred***;
- if the type is user-migrateable, then allow the application secret to be transferred under control of a user; and
- if the type is third party-migrateable, then allow the application secret to be transferred under control of a third party.

In making out the rejection of this claim, the Office argues that its subject matter is anticipated by Peterka. Applicant respectfully disagrees and traverses the Office's rejection.

Specifically, Peterka fails to disclose if the type is non-migrateable, then not allow the application secret to be transferred, as recited in this claim.

Accordingly, for at least this reason, and for reasons substantially analogous to those argued above in regard to claim 1, claim 20 is allowable.

Claims 21-29 are allowable as depending from an allowable base claim.

Claim 41 recites one or more computer readable media having stored thereon a plurality of instructions that, when executed by one or more processors of a computing device, causes the one or more processors to:

- receive a plurality of encrypted application secrets from another computing device;
- identify a first group of the plurality of encrypted application secrets that are to be decrypted under user control;
- obtain, from a user of the computing device, a passphrase;
- use the passphrase to decrypt each encrypted application secret of the first group of encrypted application secrets;
- identify a second group of the plurality of encrypted application secrets that are to be decrypted under third party control; and

- communicate with a third party to have each encrypted application secret of the second group of encrypted application secrets decrypted.

In making out the rejection of this claim, the Office argues that its subject matter is anticipated by Peterka. Applicant respectfully disagrees and traverses the Office's rejection.

Specifically, Peterka fails to disclose obtaining, from a user of a computing device, a passphrase, as recited in this claim. Also, Peterka fails to disclose using the passphrase to decrypt each encrypted application secret of the first group of encrypted application secrets, as recited in this claim.

Again, Peterka is directed to disseminating preview and/or other program content to one or more clients. Peterka further states that such dissemination is controllable via decryption keys that are communicated from the program source to the client or clients (paragraphs 0006 and 0012, *et seq* of Peterka). However, Peterka does not disclose, teach or suggest obtaining a **passphrase** from a user, or any sort of use of such a **passphrase**. In any case, Peterka is certainly lacking the particular subject matter recited by claim 41.

Accordingly, this claim is allowable.

Claim 42 is also allowable as depending from an allowable base claim.

Claim 49 (as amended) recites a method comprising [emphasis added]:

- receiving a request to transfer a plurality of application secrets from a source computing device to a destination computing device;
- identifying which one of a plurality of types of application secrets the plurality of application secrets correspond to, ***wherein one of the plurality of types of application secrets considered in the identifying is non-migrateable***;
- identifying a key associated with the one type;
- allowing the plurality of application secrets to be accessible to the destination computing device by communicating the key to the destination computing device so that the destination computing device can use the key to decrypt the plurality of application secrets.

In making out the rejection of this claim, the Office argues that its subject matter is anticipated by Peterka. Applicant respectfully disagrees and traverses the Office's rejection.

Specifically, Peterka fails to disclose identifying which one of a plurality of types of application secrets the plurality of application secrets correspond to, wherein one of the plurality of types of application secrets considered in the identifying is non-migrateable, as recited in this claim. Peterka does not disclose, teach or suggest a **non-migrateable** type of application secret in any way or for any purpose. Peterka fails to disclose one or more features as recited by claim 49.

Accordingly, this claim, as amended, is allowable.

Claims 50-51 are allowable as depending from an allowable base claim.

Claim 52 recites a method comprising [emphasis added]:

- receiving a request to transfer data from a source computing device to a destination computing device;
- checking whether the data can be transferred to the destination computing device, and if so, then checking whether the data can be transferred under control of the a user or a third party, wherein checking whether the data can be transferred comprises checking a type of the data, ***the type of the data being one of non-migrateable, user-migrateable, and third party-migrateable***; and
- receiving input from the appropriate one of the user or third party to control transferring of the data to the destination computing device.

In making out the rejection of this claim, the Office argues that its subject matter is anticipated by Peterka. Applicant respectfully disagrees and traverses the Office's rejection.

Specifically, Peterka fails to disclose checking a type of the data, the type of the data being one of non-migrateable, user-migrateable, and third party-migrateable, as recited in this claim. For at least reasons analogous to

those argued above in regard to claim 1, the § 102 rejection of claim 52 is unsupportable and must be withdrawn.

Accordingly, this claim is allowable.

Claims 53 and 55-58 are allowable as depending from an allowable base claim.

Claim 59 recites one or more computer readable media having stored thereon a plurality of instructions that, when executed by one or more processors of a source computing device, causes the one or more processors to [emphasis added]:

- receive a request to transfer data from the source computing device to a destination computing device;
- identify a type of the data;
- ***if the type is non-migrateable, then not allow the data to be transferred***;
- if the type is user-migrateable, then allow the data to be transferred under control of a user; and
- if the type is third party-migrateable, then allow the data to be transferred under control of a third party.

In making out the rejection of this claim, the Office argues that its subject matter is anticipated by Peterka. Applicant respectfully disagrees and traverses the Office's rejection.

Specifically, Peterka fails to disclose identifying a type of the data, and if the type is non-migrateable, then not allowing the data to be transferred, as recited in this claim. For at least reasons analogous to those argued above in regard to claim 20, the § 102 rejection of claim 59 is unsupportable and must be withdrawn.

Accordingly, claim 59 is allowable.

Claims 60-67 are allowable as depending from an allowable base claim.

Claim 76 (as amended) recites a method comprising [emphasis added]:

- receiving a request to transfer a plurality of secrets from a source computing device to a destination computing device;
- identifying which one of a plurality of types of secrets the plurality of secrets correspond to, ***wherein one of the plurality of types of application secrets considered in the identifying is non-migrateable***;
- identifying a key associated with the one type; and
- allowing the plurality of secrets to be accessible to the destination computing device by communicating the key to the destination computing device so that the destination computing device can use the key to decrypt the plurality of secrets.

In making out the rejection of this claim, the Office argues that its subject matter is anticipated by Peterka. Applicant respectfully disagrees and traverses the Office's rejection.

Specifically, Peterka fails to disclose identifying which one of a plurality of types of secrets the plurality of secrets correspond to, wherein one of the plurality of types of application secrets considered in the identifying is non-migrateable, as recited in this claim. For at least reasons substantially analogous to those argued above in regard to claim 49, the § 102 rejection of claim 76 is unsupportable and must be withdrawn.

Accordingly, this claim, as amended, is allowable.

Claims 77-79 are allowable as depending from an allowable base claim.

Conclusion

Applicant submits that the claims are in condition for allowance. Accordingly, Applicant requests a Notice of Allowability forthwith.

Respectfully submitted,

Dated: 8/15/06

By: _____

Lance R. Sadler
Reg. No. 38,605
(509) 324-9256